

Received & Inspected

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

MAR 17 2010

FCC Mail Room

Annual 64.2009(e) CPNI Certification for 2010

Date filed: 3/09/2010

Name of company covered by this certification: PIOV, LLC

Form 499 Filer ID: 826845

Name of signatory: Craig Sleight

Title of signatory: Vice-President

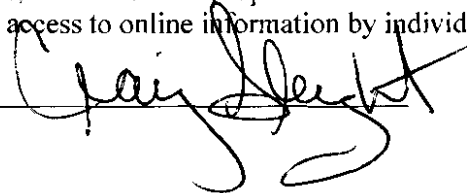
I, Craig Sleight, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules attached is a statement.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed



No. of Docs. as rec'd. 0+3
UN ARCADE

Customer Notice

CPNI Compliance Policies

Effective August 18, 2008

SinglePipe Communications, Inc.
is currently our Switch Provider

Table of Contents

Introduction	2
Process for Establishing a CPNI Authentication Passcode	3
Guidelines for Creating the Passcode	3
Service Provider Notes	4
Viewing a Customer's CPNI Passcode	4
Changing Password and/or CPNI Passcode	4
Maximum Failed Login Attempts	5
Customer (End User) Notes	6
Viewing a Customer's CPNI Passcode	6
Changing Password and/or CPNI Passcode	6
Maximum Failed Login Attempts	7
Appendix A – Procedures	8
Establishing the CPNI Passcode	8
Verifying a Customer's CPNI	8
Changing a Password	9
Changing the CPNI Authentication Passcode	10
Resetting a Forgotten Password	10

Introduction

SinglePipe Communications, Inc., and its affiliate ALEC, Inc. (together, "Company") have implemented the following policies and procedures to protect the confidentiality of Customer Proprietary Network Information ("CPNI") and to ensure compliance with the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.*, as revised by the FCC's new rules adopted in *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*.¹

CPNI is defined as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."

Company primarily provides wholesale services and support for interconnected voice-over-IP service providers and other entities. For these services, Company has knowledge of end user CPNI only insofar as it is necessary for the provisioning and maintenance of services to its wholesale customers. Company also provides certain retail services to enterprise customers.

Effective this notice date, the Company has implemented a CPNI Authentication Passcode to be used for verifying an individual customer's identity before providing access to confidential and proprietary customer information. The CPNI Authentication Passcode affects the SIPS (SinglePipe Information Provisioning System) Portal, the end user Account Portal, and support procedures. The remainder of this document explains the changes.

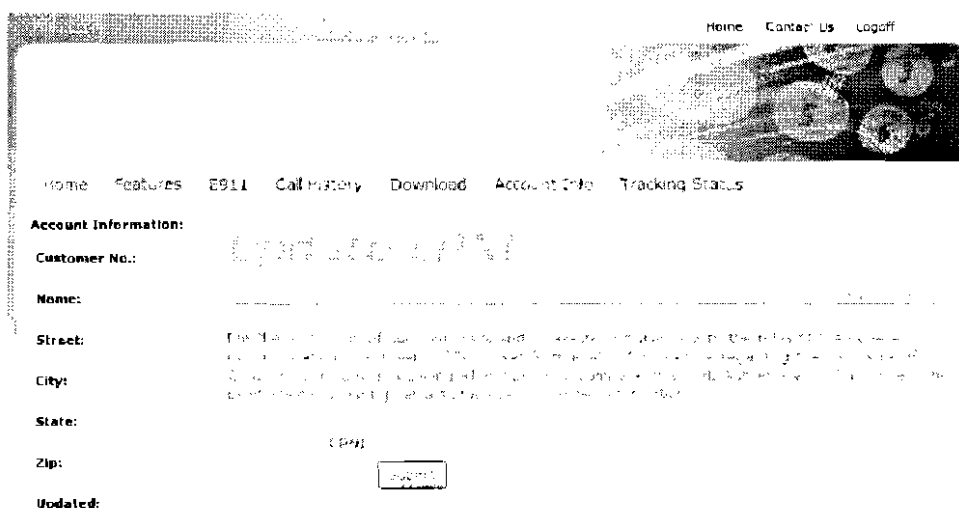
¹, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22 (rel. April 2, 2007)

Process for Establishing a CPNI Authentication Passcode

Whether an account is set up by the service provider via SIPS, or the customer signs up for telephone service via the Account Portal, the process is the same.

The customer provides an email address of record (either via the online selfregistration process, or to a CSR, who enters it in SIPS). Upon provisioning of the account, an email message is sent to the new customer's email address of record; the message includes a unique secure link to be used to activate the customer's access to his account via the Account Portal.

When the customer clicks the link, he is taken to the Account Portal, where he is prompted to create a password and CPNI Authentication Code.



The screenshot shows a web browser window with the URL "http://www.pio.com/". The page has a header with "Home", "Contact Us", and "Logoff". Below the header is a navigation bar with "Home", "Features", "E911", "Call History", "Download", "Account Info", and "Tracking Status". The main content area is titled "Account Information:" and contains the following fields:

- Customer No.:** 1234567890
- Name:** [Redacted]
- Street:** [Redacted]
- City:** [Redacted]
- State:** [Redacted]
- Zip:** [Redacted]
- Updated:** [Redacted]

Guidelines for Creating the Passcode

The Account Portal includes the following guidelines for selecting a password and CPNI passcode; they:

...should not consist of any significant portion of the customer's name, family names, account number, telephone number, street address, zip code, social security number, date of birth, other biographical or account information, or easily guessed words or strings of digits.

After the customer chooses the password and CPNI Authentication Passcode, the authentication link expires and no longer provides entry into the account.

Service Provider Notes

Wholesale service providers use SIPS to provision new accounts and to access customer account information as part of providing support.

When setting up a new account in SIPS, the wholesale service provider must enter an email address for the customer; this email address serves as the address of record for the customer's telephone account. Upon provisioning of the account, the new customer can use the email address of record and default password to access to his account via the Account Portal. Upon the initial login, the customer will be prompted to enter CPNI Passcode before he can proceed to the rest of the Account Portal.

When the customer clicks the link, he is taken to the Account Portal, where he is prompted to create a password and CPNI Authentication Code (see previous

Viewing a Customer's CPNI Passcode

Use the CPNI Passcode to verify a caller's identity when providing support. Once established by the customer, the CPNI is available in SIPS, on the Customer page as part of the contact information. Notice that it is read-only; a service provider cannot change the CPNI passcode.

Customer

Customer	Services	E911	DiDs	Email	Call History	Remarks
Jane Example - 000000						
Required fields						
Enter customer name						
Service provider name:		Agent:		Account status:		
SinglePipe_Channel				Active		
Account type:		Dwelling				
Residential						
Contact first name:		Contact last name:		MI:	Salutation:	CPNI: Portal locked-out?
Jane		Example				.1111
SSN/EIN:		Phone number:		Email address:		SP customer id:
(Make sure you enter the correct e-mail This will be the customer login username)						

Changing Password and/or CPNI Passcode

The following policies are designed to ensure security of the customer's CPNI information:

☐ Only the customer can change his or her password and CPNI Authentication Passcode via the Account Portal.

☐ The service provider cannot change a customer's password or CPNI passcode.

☐ If a customer forgets his password, he now must provide a valid username and CPNI passcode combination to have login credentials sent to the account's address of record.



Broadband Phone Service

If the customer also forgets his or her CPNI passcode, login credentials cannot be provided online. The customer must contact the Company by phone and request login credentials. Company will provide them:

- By a return telephone call to the telephone number of record for the account.
- By letter, mailed to the mailing address of record, provided this address has been on file for at least 30 days.

Maximum Failed Login Attempts

After 5 consecutive failed attempts to sign in to the Account Portal, the account will be locked to protect it from serial access attempts by an unauthorized person.

To unlock an account, the customer must call Company and provide identifying information to request that the account be unlocked. If there is an unusual number of requests to unlock an account, Company will contact the customer's telephone number of record or address of record to verify that the unlock requests were authorized by the customer.

Customer (End User) Notes

When registering for a new account via the online portal, the customer must enter an email address for the customer; this email address serves as the address of record for the customer's telephone account. Upon provisioning of the account, the new customer can use the email address of record and default password to access to his account via the Account Portal.

Upon the initial login, the customer will be prompted to enter a CPNI Passcode before he can proceed to the rest of the Account Portal (see previous section, Process for Establishing a CPNI Authentication Passcode).

Viewing a Customer's CPNI Passcode

Once established by the customer, the CPNI is available to the customer via the Account Portal. The customer can sign in to the Account Portal to view and update his or her CPNI passcode.

Account Information

Personal Info Service Address Billing Address

Customer Name:

CPNI: (111) ←

Contact Phone:

Email Address:

Update Cancel

Changing Password and/or CPNI Passcode

The following policies are designed to ensure security of the customer's CPNI information:

- ☐ Only the customer can change his or her password and CPNI Authentication Passcode via the Account Portal.
- ☐ The service provider cannot change a customer's password or CPNI passcode.
- ☐ If a customer forgets his password, he now must provide a valid username and CPNI passcode combination to have login credentials sent to the account's address of record.
- ☐ If the customer also forgets his or her CPNI passcode, login credentials cannot be provided online. The customer must contact the Company by phone and request login credentials. Company will provide them:

- By a return telephone call to the telephone number of record for the account.

- By letter, mailed to the mailing address of record, provided this address has been on file for at least 30 days.

Maximum Failed Login Attempts
--

After 5 consecutive failed attempts to sign in to the Account Portal, the account will be locked to protect it from serial access attempts by an unauthorized person.

To unlock an account, the customer must call Company and provide identifying information to request that the account be unlocked. If there is an unusual number of requests to unlock an account, Company will contact the customer's telephone number of record or address of record to verify that the unlock requests were authorized by the customer.

Appendix A – Procedures

This section includes instructions for completing the following tasks:

- ☐ Establishing the CPNI passcode (customer)
- ☐ Verifying a customer's CPNI passcode (support)
- ☐ Changing a password (customer)
- ☐ Changing the CPNI passcode (customer)
- ☐ Resetting a password (customer)

Establishing the CPNI Passcode

Using the link provided in the welcome message, access the Account Portal. You are prompted to enter a password, and then enter the CPNI for your account.

Home Contact Us Logout

Home Features E911 Call History Download Account Info Tracking Status

Account Information:

Customer No.:

Name:

Street:

City:

State:

Zip:

Updated:

CPNI

Submit

Verifying a Customer's CPNI

When a person calls in about his or her telephone account, you should verify the CPNI before proceeding further. The CPNI is available on the first page of the Customer page, with the contact information.

Customer

Customer Services: EP11 QID: Email: Call History Remarks

Jane Example - 000000

Required fields

Enter customer name

Service provider name:

Agent

Account status:

SinglePipe_Channel

Active

Account type:

Dwelling

Residential

Contact first name

Contact last name

MI:

Salutation:

CPNI:

Portal locked-out?

Jane

Example

1111

SSN/EIN:

Phone number:

Email address:

SP customer id

(Make sure you enter the correct e-mail)

This will be the customer login username)

Changing a Password

You can change the password from the Account Portal.

To update your password:

1. Sign in to the Account Portal using your username and password.
2. On the Account Info menu, click Change Password.
3. Enter your current password ("old password") and then enter a new password for your account.

4. Click **Submit**.

You can also change the CPNI Authentication Passcode from the Account Portal.

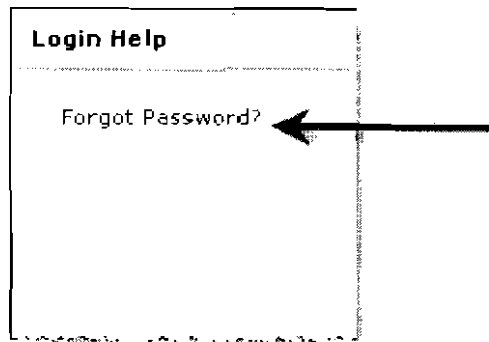
To change the CPNI:

1. Sign in to the Account Portal using your username and password.
2. On the Account Info menu, click **Update Account**.
3. On the Account Information page, make sure the **Personal Info** tab is selected, and enter a new CPNI.

4. Click **Update**.

Resetting a Forgotten Password

If you forget your password, you can request a new password from the Account Portal.



To ensure security, the reset password process now requires a valid username and CPNI passcode. After the customer enters this information, the login credentials are sent to the email address of record.

CPNI Compliance Policies of SinglePipe Communications, Inc. and ALEC, Inc.

Revision Effective June 8, 2008

SinglePipe Communications, Inc. and its affiliate ALEC, Inc. (together, “Company”) have implemented the following policies and procedures to protect the confidentiality of Customer Proprietary Network Information (“CPNI”) and to assure compliance with the rules of the Federal Communications Commission (“FCC”) set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.*, as revised by the FCC’s new rules adopted in *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22 (rel. April 2, 2007).

CPNI is “(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.”

Company primarily provides wholesale services and support for interconnected voice-over-IP service providers and other entities. For these services, Company has knowledge of end user CPNI only insofar as it is necessary for the provision and maintenance of service to its wholesale customers. Company also provides certain retail services to enterprise customers. The following summary describes Company’s policies, administered by its CPNI Compliance Manager Mark Hayes, that are designed to protect the confidentiality of its customers’ CPNI.

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

Company will use, disclose, or permit access to CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for telecommunications services; to protect the its rights or property, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide inside wiring installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

Company does not use CPNI to market service offerings among the different categories of service, or even within the same category of service, that it provides to subscribers. Company does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

In accordance with Section 222(b) of the Act, 47 U.S.C. § 222(b), when Company receives or obtains proprietary information from another carrier for purposes of providing a

telecommunications service, it will only use such information for such purpose, and does not use such information for its own marketing efforts.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

Above and beyond the specific FCC requirements, Company will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of possible new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to Company's existing policies that would strengthen protection of CPNI, they should report such information immediately to Company's CPNI Compliance Manager so that Company may evaluate whether existing policies should be supplemented or changed.

A. Inbound Calls to Company Requesting CPNI

Call Detail Information (CDI) is a subset of CPNI that includes any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

Company only provides CDI to inbound callers in accordance with the following procedures:

- Inbound caller must provide the CPNI Authentication Passcode associated with their account.
- If a customer is able to provide to the CSR the telephone number called, when it was called, and, if applicable, the amount charged for the call, exactly as that information appears on the bill, then the CSR is permitted to discuss customer service pertaining to that call and that call only. If the detail provided by the caller does not match on all categories, the CSR should not inform the caller which portion of the detail does not match (for example, they should not tell the customer there were no calls during a particular hour or that there are no calls to a particular number). CSRs are trained to recognize that a pretexter may be as interested to know about the absence of a particular call as its existence.
- A supervisor may place a call to the customer's telephone number of record. The CSR may not rely on Caller ID information to assume that the caller is calling from such number; they must disconnect the inbound call and make a new outbound call to that number.
- Company may send a copy of a bill or requested CDI to a mailing address of record for the account, but only if such address has been on file with Company for at least 30 days.

For CPNI other than CDI, CSRs are trained to require an inbound caller to authenticate their identity using methods appropriate for the information sought prior to revealing any CPNI or account information to the caller.

B. In-Person Disclosure of CPNI at Company Offices

Company may disclose a customer's CPNI to an authorized person visiting a Company office upon verifying that person's identity through a valid, non-expired government-issued photo ID (such as a driver's license, passport, or comparable ID) matching the customer's account information.

C. Notice of Account Changes

When an address of record is created or changed, except in connection with the customer's initiation of service, Company will immediately send a notice to customer's pre-existing address of record notifying them of the change. When an online account, password, and/or CPNI Authentication Passcode is created or changed, a notice will immediately be sent to customer's address of record notifying them of the change. Such notices will not reveal the changed information, and will direct the customer to notify its service provider immediately if they did not authorize the change.

D. Online Access to CPNI

When a customer submits a request for new telephone service, they must provide an email address that will serve as an address of record for their telephone account. An email is sent to the new customer's email address of record that includes a unique secure link that can be used to access on-line account through which the customer may obtain or update certain account information.

The customer is initially authenticated through the use of this link. Upon initial entry into the on-line portal through this link, the customer is required to choose a password and a CPNI Authentication Passcode. After the user chooses a password, the authentication link sent to the customer expires and no longer provides entry into the account, which thereafter can only be accessed by correctly providing the login ID and password.. The site instructs the user to select a password and Passcode that do not consist of any significant portion of the customer's name, family names, account number, telephone number, street address, zip code, social security number, date of birth, other biographical or account information, or easily guessed words or strings of digits.

A password and/or the CPNI Authentication Passcode may be changed by the user after logging into the online account with the correct login ID and password.

If a customer forgets their password, they may enter their CPNI Authentication Passcode to have their login credentials sent to their address of record. If they have also do not have their CPNI Authentication Passcode, they may only obtain these credentials by contacting company by phone and asking for these credentials to be provided by a return telephone call to the telephone number of record for the account, or sent to the address of record that has been on file for 30 days, or they may visit a Company office and present photo identification that meets the requirements of Section II.B. herein.

If there are 5 or more consecutive failed attempts at access to an online account without an intervening successful login, the account will be locked to protect it from serial access attempts by an unauthorized person. To unlock an account, the customer must call Company and provide identifying information to request that the account be unlocked. If there is an unusual number of requests to unlock an account, Company will contact the customer's telephone number of record or address of record to verify that the unlock requests were authorized by the customer.

E. Alternative Arrangements

Pursuant to 47 C.F.R. § 64.2010(g), the requirements set forth in this section III do not apply to business customer accounts (including Company's carrier customers) where the customer is able to contact a dedicated account representative and has a contract with Company that specifically addresses Company's protection of CPNI.

Company may deviate from the provisions described in this Section II for its wholesale customers on a customer-by-customer basis to permit other compliant implementations by a customer that has prepared its own written CPNI compliance plan that it has filed or will timely file in FCC Docket 06-36.

IV. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any Company employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the Company CPNI Compliance Manager, and such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is Company's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate the Company's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

A. Identifying a "Breach"

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Manager.

If a Company employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to Company's CPNI Compliance Manager who will determine whether to report the

incident to law enforcement and/or take other appropriate action. Company's Compliance Manager will determine whether it is appropriate to update Company's CPNI policies or training materials in light of any new information; the FCC's rules require Company on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."

B. Notification Procedures

As soon as practicable, and in no event later than 7 business days upon learning of a breach, the Company CPNI Compliance Manager shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: <https://www.cpnireporting.gov>. Company's FRN number and password may be required to submit a report. If this link is not responsive, they should contact counsel or the FCC's Enforcement Bureau (202-418-7450 or <http://www.fcc.gov/eb/cpni>) for instructions.

Company will not notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided below (a full business day does not count a business day on which the notice was provided). Federal law requires compliance with this requirement even if state law requires disclosure.

If Company receives no response from law enforcement after the 7th full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach. Company will delay notification to customers or the public upon request of the FBI or USSS.

If the Company Compliance Manager believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; Company still may not notify customers sooner unless given clearance to do so from *both* the USSS and the FBI.

V. RECORD RETENTION

The Company Compliance Manager is responsible for assuring that we maintain for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Company maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI. If Company later changes its policies to permit the use of CPNI for marketing, it will maintain a record, for at least one year, of supervisory review of marketing that proposes to use CPNI or to request customer approval to use or disclose CPNI.

Company will have an authorized corporate officer, as an agent of both SinglePipe and ALEC, sign a compliance certificate on an annual basis stating that the officer has personal knowledge

that SinglePipe and ALEC have established operating procedures that are adequate to ensure compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC Enforcement Bureau in EB Docket No. 06-36 by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how Company's operating procedures ensure compliance with the FCC's CPNI rules. In addition, the filing must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. Confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

VI. TRAINING

All employees with access to CPNI receive a copy of Company's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, Company Bresnan conducts mandatory CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, and marketing personnel. The CSR training emphasizes, among other points, that CSRs be cognizant that some unauthorized persons may have significant apparent familiarity with a customer's biographical and account information.